



Qualis A3 ISSN: 2178-2008

ARTIGO

## Revista Processus de Estudos de Gestão, Jurídicos e Financeiros



### Personal Data Protection and Cybersecurity in Algerian Legislation

Himeur Zelikha<sup>1</sup>

<https://orcid.org/0009-0006-3805-7151>

PhD, Faculty of Law and Political Science,  
University of 08 May 1945, Guelma, Algeria  
Email: z.himeur10@gmail.com



#### Publication Information

ISSN: 2178-2008

Received: 18-01-2026

Accepted: 26-03-2026

Published: 01-04-2026

#### Keywords:

Algeria  
Cybercrime  
Cybersecurity  
Data Protection  
Digital Rights  
Personal Data.

#### Abstract

Algerian society is witnessing an increase in cybersecurity threats due to the growing reliance on digitalization, making the protection of personal data a central pillar for ensuring fundamental individual rights, which are intertwined with the use of modern technologies and digital security requirements. Through Law No. 18-07, the Algerian legislator attempted to regulate the processing of personal data and ensure its confidentiality. However, this legislation faces tangible challenges in establishing a substantive balance between privacy protection and the requirements of the digital sphere, particularly in light of the proliferation of cybercrime and the growth of digital data surveillance. The importance of the National Authority for Data Protection emerges as a supervisory tool to balance individual rights with the necessities of national security. Despite legislative efforts, this balance remains fragile and needs reinforcement through the development of more effective legal and technical mechanisms. The study of this topic reveals the limitations of the current legislation and highlights the need for a future revision aimed at strengthening the protection of individual rights without compromising cybersecurity.

### 1. Introduction

The Universal Declaration of Human Rights of 1948 established special protection for the lives of individuals, their families, and their homes, emphasizing the necessity of respecting privacy and correspondence, and everything that could affect their reputation and honor. It stipulates that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation, and that everyone has the right to the protection of the law against such interference or attacks (United Nations, 1948, art. 12).

Building on this framework, the principle of the right to the protection of personal data was enshrined in Algerian legislation, similar to other comparative legislations. This is clearly demonstrated in the highest text of the Algerian legal system: the Constitution. The Constitution affirms the necessity of respecting the rights of others, particularly regarding the right to honor, private life, and the protection of the family, childhood, and youth (Presidential Decree No. 20-442, 2020, art. 81).

<sup>1</sup> PhD, Faculty of Law and Political Science, University of 08 May 1945, Guelma, Algeria (2003); a Master's degree in Law from Mentouri Brothers University Constantine 1 (UFMC1), Constantine, Algeria. (2017); a PhD in Law from University of 08 May 1945, Guelma, Algeria (2022).



In the same context, Article 47 of the Constitution reinforces individual freedoms and safeguards the dignity of the citizen in line with contemporary developments, stating: "The protection of individuals in the processing of personal data is a fundamental right. The law punishes any violation of these rights" (Presidential Decree No. 20-442, 2020, art. 47).

Therefore, the protection of natural persons in the context of processing personal data is a fundamental right guaranteed by law, whose violation is punishable. This right is no longer presented within its traditional narrow framework but has become closely linked to the profound transformations brought about by rapid technological development, especially in information and communication technologies and the spread of social networks that have brought millions of people closer together and created new opportunities for accessing and exchanging information. Personal data has become easily tradable through the collection and storage of information using the latest and most dangerous devices modern science has developed for capturing and transmitting images, wiretapping, recording, and even investigating and searching through information and images, as well as big data processing software that has enabled global companies to trade in individuals' data and exploit it for advertising, informational, and other economic purposes.

Consequently, the spread of digital systems and massive databases has led to an unprecedented expansion in the collection, processing, and storage of personal data, exposing it to multiple risks such as cyberattacks, unlawful intrusions, and data misuse. This situation has made the legal protection of such data an absolute necessity, linked to the effectiveness of the adopted cybersecurity mechanisms, especially as it now forms the connecting link between technological development and privacy protection, not merely a legislative choice.

This situation requires the legislator to adopt a comprehensive approach that integrates legal rules and technical measures to achieve a balance between the demands of digital transformation and the necessity of safeguarding individual rights and freedoms.

Thus, the central question arises: Has the Algerian legislator succeeded in establishing a substantive balance between the protection of personal data as a manifestation of fundamental individual rights and the requirements of cybersecurity, which expose the collection and processing of data to risks while aiming to ensure the safety of individuals and society?

To answer this research problem, this study is divided into two sections. The first section examines the legal framework for the protection of personal data in Algeria, while the second section is dedicated to studying the challenges of cybersecurity and their impact on the protection of personal data in Algeria.

## **2. The Legal Framework for the Protection of Personal Data**

The rapid evolution in the field of information technology has given rise to a new legal reality where personal data constitutes a fundamental pillar in various digital transactions, especially with the increasing use of computers and the internet in public and private institutions within the framework of automated processing of personal data. This reality has resulted in increased risks of intrusion into the private life of individuals, which necessitated legislative intervention to adopt a protective framework ensuring effective protection for this data. The situation is no longer merely a technical or scientific matter but has become linked to the individual's right to privacy.



Therefore, we will address the manifestations of this legal enshrinement that regulates and governs the processing of personal data (Section 2.1), leading to an explanation of the legal guarantees for the protection of personal data (Section 2.2).

## **2.1. The Legal Enshrinement of Personal Data Protection**

The legal enshrinement of personal data protection manifests as a practical response to the real risks generated by the intensive use of information technology. The risks are no longer hypothetical but have materialized into concrete instances of unlawful exploitation of personal data. This necessitated legislative intervention to establish effective legal protection for this data, both at the national and international levels, which will be addressed in the following subsections.

### **2.1.1. The Legal Enshrinement of Personal Data Protection at the National Level**

Personal data concerning an individual includes information falling under the protection of the constitutional right to privacy, such as name, gender, blood type, religion, address, marital status, educational qualifications, and profession. This data identifies the individual and dispels any uncertainty about their identity. It also includes civil facts—elements of the individual's civil status such as marriage, divorce, nationality, residence, death, and national identification number—as well as financial and occupational information like monthly income and debts (Rafi', 2018, p. 91).

Given the sensitive nature of this data, the Algerian legislator, like comparative legislations, has sought to protect it in general, starting from the highest state document, considering the protection of personal data as a fundamental right guaranteed to every individual. This enshrinement was reinforced by the enactment of Law No. 18-07 on the protection of personal data, in addition to the Penal Code and the Child Protection Law, which are presented sequentially.

#### **2.1.1.1. In the Algerian Constitution**

The Algerian Constitution of 2020 (Presidential Decree No. 20-442, 2020) serves as the constitutional basis for the protection of personal data, enshrining the right to private life and the sanctity of individuals, and guaranteeing the confidentiality of correspondence and communications in all their forms (Presidential Decree No. 20-442, 2020, art. 34, para. 2 & art. 47), including modern digital communications. In other words, personal data is an extension of the private life of individuals and cannot be infringed upon except in accordance with the law (Presidential Decree No. 20-442, 2020, art. 34, para. 2). This reflects a clear intention to protect the private lives of individuals from the risks of the unlawful use of information technology.

#### **2.1.1.2. In Law No. 18-07 on the Protection of Personal Data**

Reinforcing this constitutional approach, the Algerian legislator enacted Law No. 18-07 on the protection of natural persons with regard to the processing of personal data (Law No. 18-07, 2018). This law defines the concept of personal data (Law No. 18-07, 2018, art. 3), organizes and controls the conditions for its collection and processing, and establishes the principle of prior consent as a condition for the lawfulness of processing personal data. Consent is defined as a free, specific, informed, and unambiguous indication of the data subject's wishes by which they agree to the collection and processing of their data for a specific lawful purpose (Law No. 18-07, 2018, art. 7).



Furthermore, the aforementioned law obliges the data controller (Law No. 18-07, 2018, arts. 22-31) to take the necessary technical and organizational measures to ensure the security and confidentiality of the data, its deletion or modification, and its use without the owner's authorization. All data stored or processed within information systems becomes legally protected and cannot be breached or used unlawfully (Law No. 18-07, 2018, arts. 38-41).

Notably, the Algerian legislator strengthened the protection mechanisms by establishing a specialized institution—the National Authority for the Protection of Personal Data—as an independent body representing the legal reference for monitoring the implementation of personal data protection legislation. It receives complaints, grants authorizations, and thus demonstrates the transition from theoretical protection to actual, practical, institutional protection. The Authority takes various procedural actions, ranging from warnings and notices to temporary or, in some cases, permanent withdrawal of the declaration receipt or authorization, depending on the gravity of the violation committed by the data controller, or imposes financial penalties. These measures taken against the data controller are subject to appeal before the Council of State (Law No. 18-07, 2018, arts. 46-48).

Thus, the National Authority for the Protection of Personal Data serves as an official point of contact between individuals and data processing entities, enhancing the preventive and subsequent mechanisms for protecting individual rights.

### **2.1.1.3. In Other Laws**

#### **2.1.1.3.1. In the Algerian Penal Code**

The Penal Code (Law No. 04-15, 2004) established a legal framework for the protection of personal data against digital assaults, criminalizing any act involving unlawful access to information systems (Amieur, 2022, p. 96). It also introduced a set of substantive legal rules defining acts that affect automated data processing systems. This includes offenses against automated data processing systems in their simple form, such as unauthorized access using technical means, where the act of access itself is not necessarily unlawful but becomes criminalized because it was carried out without right or authorization (Qara, 2007, p. 106), provided the unauthorized access is intentional and not accidental or erroneous. It also includes remaining unauthorized within the automated data processing system, which involves continuing to be present in the system without the permission of its owner or controller (Law No. 04-15, 2004, art. 394 bis).

In addition, there is an aggravated form of the offense against automated data processing systems, where the penalty is increased if the act results in the deletion or alteration of system data or hinders the system's functioning (Law No. 04-15, 2004, art. 394 bis, para. 2).

#### **2.1.1.3.2. In the Child Protection Law**

Law No. 15-12 on the protection of the child (Law No. 15-12, 2015) establishes special protection for a child's personal data, recognizing them as a vulnerable group requiring enhanced legal care. It guarantees the child's right to respect for their private life and human dignity, prohibiting all forms of intrusion into the child's identity, image, or reputation, particularly through publication, circulation, or exploitation, especially if the child is in a dangerous situation or is a crime victim (Law No. 15-12, 2015, art. 141). The scope of this protection extends to the digital space and modern media, safeguarding against the risk of publishing or broadcasting any information that could enable others to identify the child, exploit their personal data, or defame them (Ben Dhiab, 2012, p. 281).



The legislator granted juvenile judges broad powers to take preventive and urgent measures to stop any violation of the child's privacy, including ordering the blocking of harmful digital content (Law No. 15-12, 2015, art. 141).

Thus, the Algerian legislator has sought to provide effective legal protection against the digital exploitation of children's personal data.

### **2.1.2. The Legal Enshrinement of Personal Data Protection at the International Level**

The protection of personal data has become a fundamental human right as a result of technological development and digital transformation, closely linked to the right to privacy. The urgent need to conclude international agreements to protect these rights has emerged. The following are some key international instruments.

#### **2.1.2.1. The Universal Declaration of Human Rights (1948)**

Although it does not explicitly mention "personal data," Article 12 of the Universal Declaration of Human Rights of 1948 (United Nations, 1948, art. 12) established indirect protection, stating that no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor and reputation. This text serves as the first reference framework for the protection of informational privacy (Jabbour & Jabbour, 2018, p. 24).

#### **2.1.2.2. The International Covenant on Civil and Political Rights (1966)**

Article 17 of the International Covenant on Civil and Political Rights of 1966 (United Nations, 1966, art. 17) states that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation. The efforts of the United Nations Human Rights Committee have interpreted this article to include electronic personal data.

#### **2.1.2.3. Regional International Agreements**

The European Union - General Data Protection Regulation (GDPR) is a unified European law aimed at protecting the privacy of personal data of EU citizens by regulating the collection, processing, storage, and transfer of personal data, and ensuring individuals' rights to control their data. It represents one of the strongest international legislative models for personal data protection (Regulation (EU) 2016/679, 2016). This regulation was adopted on April 14, 2016, and became enforceable on May 25, 2018, granting users the right to have their data partially or completely erased from the internet. It establishes fundamental principles such as lawfulness, transparency, and purpose limitation, alongside broad rights for data subjects, including the rights to access, rectification, and erasure, making it an international reference for many comparative legislations (European Union Agency for Fundamental Rights, 2012).

The Role of International Organizations in Protecting Personal Data: The International Telecommunication Union (ITU), a specialized UN agency, works to develop telecommunications and information and communication technologies across 194 member states. It has established technical and legal standards to ensure the security of communication networks and data during transmission and processing, thereby protecting individuals in an increasingly complex digital environment (United Nations Office at Geneva, n.d.).



The Arab Convention on Combating Information Technology Offenses: This is the first regional Arab instrument aimed at unifying and strengthening the legislative, judicial, and security efforts of Arab states in combating information technology offenses, particularly concerning the right to privacy and the protection of personal data (League of Arab States, 2010, art. 1). The convention criminalizes acts such as unlawful access to information systems, unlawful interception of data, and the misuse or disclosure of personal data (League of Arab States, 2010, arts. 5-9). As such, it complements international frameworks focused on the legislative and regulatory aspects of the digital environment.

Therefore, the legal enshrinement of personal data protection, both nationally and internationally, is not merely the product of doctrinal evolution but a response to real-world situations revealed by a complex digital environment. This has reinforced the protection of personal data by unifying international standards in this field, making it both a legal and security necessity.

## **2.2. Legal Guarantees for the Protection of Personal Data**

The system for protecting personal data in Algerian legislation relies on a set of guarantees to establish a balance between the right and interest of individuals in protecting their private lives and the interest of entities in using data for legitimate purposes.

To strengthen the legal and preventive protection framework, a set of rights has been enshrined for the data subject, while a set of legal obligations is imposed on the data controller. This will be clarified in the following subsections.

### **2.2.1. The Rights of the Data Subject as a Protective Guarantee**

Recognizing the rights of the data subject is one of the most important legal guarantees, enabling them to control their data and prevent its arbitrary and unlawful use. The Algerian legislator addressed the rights of the data subject in Title IV, specifically in Articles 32 to 37. These rights include the right to information, the right of access, the right to rectification, the right to object, and the prohibition of direct marketing prospecting.

1. **The Right to Information:** The legislator obliges the data controller or their representative to provide prior, explicit, and unambiguous information to any person contacted for the purpose of collecting their personal data, particularly regarding the identity of the data controller and the purposes of the processing (Law No. 18-07, 2018, art. 32, para. 3). If information is collected on open networks, the data subject must be informed and alerted that their data is on the networks and could be exploited without their authorization (Law No. 18-07, 2018, art. 32, para. 3). It is worth noting that the obligation to inform is waived only when it is impossible to inform the data subject. The legislator limited this to three cases: processing for statistical, historical, or scientific purposes, provided reasons for the impossibility are submitted to the national authority; processing required by legal provision; and processing carried out solely for journalistic, artistic, or literary purposes (Law No. 18-07, 2018, art. 33).
2. **The Right of Access:** The law grants the data subject the right to access their personal data, including whether or not their data is being processed, the purposes of the processing, the categories of data concerned, and the recipients. This provides the data subject with all available information regarding the source of the



data (Law No. 18-07, 2018, art. 34, paras. 1-2). Conversely, the legislator allows the data controller to request that the national authority set deadlines for responding to legitimate access requests and also grants them the right to object to frivolous requests (Law No. 18-07, 2018, art. 34, para. 3).

3. **The Right to Rectification:** The legislator recognizes the data subject's right to obtain the updating, rectification, erasure, or blocking of personal data whose processing is inaccurate or incomplete, ensuring the integrity of the data being processed under Law No. 18-07. The data controller is required to make the necessary corrections free of charge for the applicant within ten (10) days of notification. If no response is received, the data subject may file a request with the national authority (Law No. 18-07, 2018, art. 35, para. 1). It is noteworthy that any third party who received the personal data must be notified of any update or correction, and upon the death of the data subject, the right passes to their heirs (Law No. 18-07, 2018, art. 35, para. 2).
4. **The Right to Object:** The legislator grants the data subject the right to object to the processing of their personal data, especially for commercial or promotional purposes, or in cases of unlawful processing. The legislator makes an exception, stating that the data subject cannot object when the processing is based on a legal obligation or an explicit provision in the document processing the data (Law No. 18-07, 2018, art. 36).
5. **Prohibition of Direct Marketing Prospecting:** This is a prominent manifestation of the right to object. It consists of the data subject's right to prevent the use of their data for direct marketing prospecting by any means without their consent. Importantly, every individual has the right to refuse to receive advertisements or commercial offers, object to the use of their mobile phone number or email for marketing purposes, and demand the immediate cessation of such communications (Law No. 18-07, 2018, art. 37; Nassakh, 2021, pp. 61-62). For example, if a telecommunications company uses a person's phone number to send advertising offers without their consent, they can object to this use, demand the company delete their number from its database, and if the situation persists, they can resort to the competent authority.

These rights constitute fundamental legal guarantees that enable the data subject to exercise effective control over their personal data, strengthening protection against any arbitrary or unlawful exploitation.

### **2.2.2. The Obligations of the Data Controller as a Preventive Guarantee**

Law No. 18-07 on the protection of natural persons with regard to the processing of personal data defines the obligations of the data controller, which form the cornerstone of the privacy protection system amidst this digital transformation. It also holds them civilly and criminally liable for any breach of their obligations.

**First: The Obligation of Lawfulness:** The processing of personal data must be based on a lawful legal basis, which involves taking the necessary technical measures and precautions to protect and secure personal data against hacking, damage, and any unlawful use, especially if transmitted over a specific network. These measures increase proportionally with the value of the data. If the data controller uses another processor (subcontractor), the latter must provide sufficient guarantees regarding the security and integrity of the personal data. This subcontracting must be based on a written contract or legal instrument, and the subcontractor may only act according to the instructions and



directions of the primary data controller (Law No. 18-07, 2018, arts. 38-40; Nassakh, 2021, p. 62).

Second: The Obligation of Confidentiality: The data controller and all persons who have access to personal data are bound by professional secrecy, even after the termination of their functions (Law No. 18-07, 2018, art. 40).

Third: Processing Personal Data in the Context of Electronic Certification and Electronic Communications: Electronic certification services involve issuing electronic certificates (Al-Obaidi, 2012, p. 179) to the signatory based on their personal data. This necessitates intervention to protect them by imposing a set of procedures that serve as a strong guarantee for those dealing with these entities, particularly regarding personal data protection, to achieve a certain level of security and trust in electronic signatures. Therefore, these personal data may not be processed except for the purposes for which they were collected, except with the explicit consent of the owners (Law No. 18-07, 2018, art. 42). Similarly, electronic communications service providers are required to inform the national authority and the data subject in case of damage, loss, disclosure, or unauthorized access, especially in public spaces. They are obligated to log any digital infringement affecting personal data (Law No. 18-07, 2018, art. 43).

Fourth: Transfer of Data to a Foreign Country: The transfer of personal data is one of the most sensitive issues in data protection due to the potential risks it poses to state sovereignty and the fundamental rights of individuals. Transferring data to a foreign country means any transmission or making available of personal data to a foreign country or international organization, whether by electronic or other means (Law No. 18-07, 2018, arts. 44-45). The transfer of personal data to a foreign country is permitted only if that country ensures an adequate level of protection. Exceptions are allowed in specific cases, including the explicit consent of the data subject, if the transfer is necessary for the data subject's life, for safeguarding the public interest, or to comply with obligations that allow the establishment, exercise, or defense of a right before the courts (Law No. 18-07, 2018, arts. 44-45).

The rights and obligations related to personal data protection constitute fundamental pillars for ensuring respect for the privacy of individuals and enhancing trust in digital transactions amidst the rapid development of information and communication technologies. Achieving a balance between the personal rights of data subjects and the requirements of lawful data processing remains contingent on the effective implementation of oversight mechanisms to prevent any arbitrary use of personal data.

### **3. Challenges of Cybersecurity and Their Impact on the Protection of Personal Data in Algeria**

The rapid development of information and communication technologies has led to profound and accelerated transformations in the methods of collecting, processing, and storing personal data, making cyberspace a fertile ground for threats and cyberattacks that pose a real threat to individuals' privacy and data security.

In light of the expanding use of digital platforms across various vital sectors, the Algerian legislator faces a dual challenge: meeting the requirements of personal data protection while ensuring cybersecurity. This necessitates an examination of the nature of these challenges in Section 3.1 and the mechanisms for strengthening cybersecurity protection for personal data in Section 3.2.



### **3.1. The Nature of Cybersecurity Challenges in Protecting Personal Data**

The evolution of cyber threats, now encompassing complex patterns of electronic attacks targeting digital infrastructures and databases, is no longer limited to traditional criminal acts. These challenges intersect with organizational and human dimensions, such as limited cybersecurity awareness. The importance of understanding the nature of these challenges lies in analyzing their essence by defining cybersecurity, which will be covered in Subsection 3.1.1. Subsection 3.1.2 is dedicated to studying the technical and organizational challenges in securing personal data, as this is the primary entry point for understanding their impact on the effectiveness of the legal protection of personal data.

#### **3.1.1. The Concept of Cybersecurity and Its Importance in Protecting Personal Data**

Cybersecurity is defined as the practice of defending computers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also referred to as the security of networks, information systems, data, information, and internet-connected devices (Jabbour, 2016, p. 25). Edward Amoroso (2007, p. 1) defined it as the means to reduce the risk of attacks on software, computer hardware, or networks, including tools used to counter hacking and detect viruses.

Thus, cybersecurity can be described as the sum of technical, organizational, and legal measures aimed at protecting information systems, networks, and databases from various electronic threats and attacks, while also ensuring the confidentiality, integrity, and availability of data.

It is noteworthy that the Algerian legislator addressed cybercrime through provisions related to the prevention of offenses connected with information and communication technologies. The legislator has not settled on a single term for these crimes. They were referred to as "crimes against automated data processing systems" under Law No. 04-15 (Penal Code). Then, under Law No. 09-04 on the prevention and fight against offenses connected with information and communication technologies, the term "offenses connected with information and communication technologies" was used, defined as "crimes against automated data processing systems as defined in the Penal Code and any other crime committed or facilitated through an information system or electronic communications network" (Law No. 09-04, 2009, art. 2, para. 1). It can be observed from this definition that it broadly and comprehensively defines the scope of these crimes, encompassing all new developments arising from technological advancements.

Consequently, the legislator views cybersecurity from a deterrent perspective, primarily based on criminalization and punishment, rather than as a comprehensive system for prevention and securing personal data. This legislative approach in Algeria has a direct impact on personal data protection, as the absence of a legal framework for cybersecurity leads to a lack of defined preventive obligations on data controllers, making legal protection contingent on ex-post intervention after a violation has occurred, rather than adopting a proactive approach that prevents infringements on personal data. Thus, the deterrent approach dominates over the preventive one.

Therefore, a computer crime is defined in technical terms as a type of criminal activity where computer technology is used directly or indirectly to achieve the intended criminal act (Adnan, 2013, p. 433).



### 3.1.2. Technical and Organizational Challenges in Securing Personal Data

Despite the critical importance of cybersecurity, its achievement faces several technical and organizational challenges that affect and limit the effectiveness of the legal protection of personal data.

First: At the Technical Level

Samir Bara (2017, p. 260) summarized the most serious threats faced by states into four types: service disruption, information destruction or alteration, network espionage, and the destruction of assets and information. The technical challenges to cybersecurity affecting the world as a whole also affect Algeria, given the ongoing and comprehensive digitalization of all vital sectors. These challenges can be summarized as follows:

- The increasing number of internet and social media users in Algeria, exceeding 10 million subscribers, increases potential risks and negatively impacts the process of identifying the perpetrators of electronic crimes.
- The proliferation of high-speed internet technologies (ADSL/VSAT/SDSL) poses a challenge to keeping pace with the speed of life and equipping with appropriate hardware and software.
- Wireless internet (Wi-Fi/3G/4G/5G) also presents an obstacle to combating cybercrime.
- The use of proxy servers while using the internet is classified among the greatest challenges and obstacles faced by cybercrime-fighting agencies (Ben Berghouth, 2023, p. 451).

Second: At the Organizational Level:

This can be summarized as:

- Lack of coordination between states and governments due to the specific nature of cybercrime, allowing perpetrators easy access to information systems and the secrecy of information, making it difficult to disclose the nature of programs used for protection and share them with other states.
- Difficulty in adapting deterrent laws against computer crime, activating them, and implementing them in parallel with the evolution in technology, virtual identities, the sophistication of concealment techniques, and stealth viruses.
- The technical expertise of Algeria and third-world countries in the field of communication and information technology, given the dominance and monopoly of advanced technologies by developed countries (Centre de Recherche sur l'Information Scientifique et Technique, n.d.).

Furthermore, it is essential to note the lack of awareness and training in cybersecurity among users and employees as a major factor exacerbating risks, as human error often constitutes a direct cause of personal data breaches (Ministry of Health of Algeria, 2024).

Thus, cybersecurity forms the cornerstone of personal data protection; however, its effectiveness remains contingent on the ability to overcome the technical and organizational challenges that hinder the security of personal data.

### 3.2. Mechanisms for Enhancing Cybersecurity Protection for Personal Data

Algeria, like other countries around the world, has sought to strengthen its cybersecurity protection mechanisms for personal data by adopting a comprehensive national cybersecurity strategy. This underscores that cybersecurity mechanisms represent, at their core, effective solutions to limit and counter cyber threats that infringe upon human dignity and freedom. This section addresses the dimensions of Algerian public security policy in light of current cyber threats. Subsection 3.2.1 studies the



strategic dimensions, while Subsection 3.2.2 is devoted to studying the practical dimensions.

### 3.2.1. Strategic Dimensions of the Algerian Cybersecurity Policy

This subsection focuses on identifying the strategic framework adopted by the Algerian state to confront cyber threats affecting personal data. This is done through enacting specific legislation and establishing specialized institutional structures aimed at preventing digital risks, regulating the processing of personal data, and ensuring its protection, thereby establishing a proactive approach to cybersecurity through the interaction of the institutional and legislative dimensions in strengthening cybersecurity.

#### First: The Institutional Dimension of the Algerian Cybersecurity Policy

This dimension relies on the creation of specialized institutions and bodies with defined competencies, contributing to enhanced cooperation mechanisms among them to ensure the protection of the national cyberspace and secure sensitive information systems and data, especially since cyber threats are no longer limited to individuals but their danger has extended to affect digital sovereignty. This necessitates studying national cybersecurity, summarized as follows:

1. The High Security Council: An advisory body to the President of the Republic, competent in all matters of national security, including cyber threats (Constitution of 1976, 1976, art. 125).
2. The National Council for the Security of Information Systems: Competent to decide on the elements of the national strategy for the security of information systems, approve electronic certification policies, classify information systems, and provide binding opinions on relevant draft laws. It operates under the authority of the Minister of National Defense (Presidential Decree No. 20-05, 2020, art. 3, para. 2 & art. 4).
3. The National Agency for the Security of Information Systems: A public institution of an administrative nature, with key tasks including conducting digital investigations into cyberattacks, collecting, analyzing, and evaluating data to secure the facilities of national institutions, and ensuring electronic vigilance (Presidential Decree No. 20-05, 2020, art. 3, para. 3).
4. The National Gendarmerie: Includes:
  - The Center for the Prevention of Computer Crimes: Analyzes computer crime data, identifies perpetrators, and secures information systems (Melouki & Djilali, 2025, p. 219).
  - The National Institute of Forensic Science and Criminology: Coordinates with its IT department to monitor and track hacking and intrusion operations (Presidential Decree No. 04-183, 2004, art. 4; Bara, 2017, pp. 271-272).
5. The General Directorate of National Security: Includes:
  - The Central Unit for Combating Cybercrime: Integrated into the Judicial Police Directorate in 2015, it investigates cybercrimes (Melouki & Djilali, 2025, p. 219).
  - The National Body for the Prevention and Fight against Offenses Connected with Information and Communication Technologies: Its key functions include proposing elements of the national strategy for the prevention and fight against offenses connected with information and communication technologies (Presidential Decree No. 15-261, 2015, art. 8, para. 4).

#### Second: The Legislative Dimension of the Algerian Cybersecurity Policy



The legislative dimension is a cornerstone of building a cybersecurity policy, providing the legal framework governing the use of cyberspace to ensure a balance between security requirements and the protection of rights and freedoms. This has occurred in stages reflecting technological development and the growth of threats. Initially, computer programs were considered literary works protected by Ordinance No. 03-05 on Copyright and Related Rights (Ordinance No. 03-05, 2003). This was followed by Law No. 04-15, amending the Penal Code by introducing the concept of automated data processing systems. Subsequently, Law No. 06-23 expanded the scope of criminalization to include unauthorized access or presence in an information system (Law No. 06-23, 2006). This culminated in the issuance of Law No. 09-04 on the specific rules for the prevention and fight against offenses connected with information and communication technologies (Law No. 09-04, 2009), which established a set of preventive and procedural mechanisms to combat cybercrime (Law No. 09-04, 2009, arts. 4, 11-12 for preventive measures; arts. 5-7, 15 for procedural measures).

Therefore, the effectiveness of personal data protection in the face of cyber threats is achieved by strengthening coordination between institutional structures and legal texts.

### **3.2.2. Practical Dimensions of the Algerian Cybersecurity Policy**

The practical dimension represents a fundamental pillar in the success of the cybersecurity policy, reflecting the effectiveness of the legal and institutional framework as priorities of Algerian cybersecurity policy. This is achieved through practical application, capacity building, enhancing security awareness on one hand, and adopting modern technical solutions to counter cyberattacks on the other.

#### **First: The Human Dimension of the Algerian Cybersecurity Policy**

The human element represents the first and last line of defense against digital threats if properly trained; conversely, it can be the weakest link if not adequately trained and developed. Algeria recognizes this crucial importance and has created an infrastructure for training national cadres and enhancing cybersecurity awareness among various segments of society and its institutions. This is done through specialized training courses, such as those for the health sector in June 2024 (Ministry of Health of Algeria, 2024). A partnership was also established to strengthen culture and develop competencies and skills in the field of cybersecurity between the Algerian Banking Training Institute and Kaspersky Lab in April 2025 (Eco-Algeria, 2025). This demonstrates openness to international expertise to raise the level of local competencies and spread digital awareness among clients. There are also ongoing efforts to integrate cybersecurity into the educational and academic systems (Ministry of Higher Education and Scientific Research, 2026), recognizing it as a necessary challenge arising from the digital world.

#### **Second: The Technological Dimension of the Algerian Cybersecurity Policy**

Algeria is working to enhance its technical capabilities, especially with the trend towards adopting fifth-generation (5G) technologies and the profound transformations accompanying it. News reports indicate the existence of a national cybersecurity strategy based on the principles of strengthening digital sovereignty, building resilient systems, and supporting government digitalization efforts (TadomSaNews, 2025). It is worth noting that Algeria signed a bilateral agreement with Russia in the field of cybersecurity, representing a new strategic direction to strengthen digital protection and confront successive cyber threats (TadomSaNews, 2025). This agreement aims to support cyber infrastructure and develop digital defense capabilities in both countries.



Furthermore, alongside the policy of cooperation with international technology companies to develop cybersecurity innovations, it is necessary to implement technological procedures that build early detection systems for cyberattacks such as viruses, malware, and network intrusions, on one hand, and ensure encryption and authentication technologies that protect personal data during transmission and storage, complemented by backup systems to ensure data recovery in the event of a cyberattack, on the other hand (Law No. 15-04, 2015, arts. 2, para. 8-9 for encryption; Amazon Web Services, n.d., for backup).

Thus, the strategic and practical dimensions of the Algerian cybersecurity policy represent the cornerstone for activating the legislative, institutional, human, and technological frameworks. They transfer protection from the level of legal texts to the level of field application, where both the human dimension (enhancing cyber awareness) and modern technologies are crucial to ensure the prevention or minimization of cyber threats.

#### 4. Conclusion

In conclusion, the governance of personal data protection in contemporary Algeria is a fundamental pillar for ensuring a balance between benefiting from the digital transformation and safeguarding individual rights, especially in light of cybersecurity challenges and the growing risks associated with intrusions and data leaks. These risks have enabled the collection and exploitation of data by third parties for other purposes, constituting a real assault on the privacy of individual rights and the security of their personal data. Algeria has adopted a comprehensive cybersecurity strategy by establishing the national system for the security of information systems in January 2020. Despite the legislative and institutional efforts made, the effectiveness of this governance remains contingent on strengthening practical mechanisms, particularly by building an integrated and flexible system that responds to rapid developments in cyberspace. This requires updating the legal framework to keep pace with the use of artificial intelligence technologies on one hand, and spreading cyber awareness among various segments of society, whether ordinary users or those responsible for security policy, including judges, to ensure the building of a secure and trusted digital environment.

#### 5. References

1. Adnan, S. (2013). Intihāk ḥurmat al-ḥayāh al-khāṣṣah ‘abra al-intarnit [Violation of privacy online]. *Journal of Damascus University for Economic and Legal Sciences*, 29(3), 421-444.
2. Algerian Ministry of Higher Education and Scientific Research. (2026, February). *Various platforms for entrepreneurship and doctoral studies*. [List of platforms].
3. Algerian Ministry of Health. (2024, June 2-6). *Dawrah takwīnīyah ḥawla amn al-bayānāt al-ṣiḥḥīyah* [Training course on health data security] [Facebook post]. Facebook. <https://www.facebook.com/saouteDZA/posts/781511607498771>
4. Al-Obaidi, U. B. G. (2008). Ḥimāyat al-ḥaqq fī al-ḥayāh al-khāṣṣah fī muwājahat al-ḥāsib al-ālī wa-al-intarnit [Protecting the right to privacy in the face of computers and the internet]. *Arab Journal for Security Studies and Training*, 23(46), 53-82.
5. Al-Obaidi, U. B. G. (2012). Al-taṣdīq al-iliktrūnī wa-taṭbīqātuhu fī al-niẓām al-Sa‘ūdī [Electronic certification and its applications in the Saudi system]. *Al-Majallah al-Qaḍā’īyah* [Judicial Journal], \*4\*(1433), 177-220.
6. Amazon Web Services. (n.d.). *What is backup?* Retrieved February 1, 2026, from <https://www.aws.amazon.com/>
7. Amieur, R. (2022). Al-jarīmah al-iliktrūnīyah wa-ālīyāt mukāfaḥatihā fī al-tashrī‘ al-Jazā’irī [Cybercrime and its combating mechanisms in Algerian legislation]. *Academic Journal of Legal and Political Research*, 6(1), 90-112.



8. Amoroso, E. (2007). *Cyber security*. AT&T Inc.
9. Bara, S. (2017). Al-amn al-saybirānī fī al-Jazā'ir: al-siyāsāt wa-al-mu'assasāt [Cybersecurity in Algeria: Policies and institutions]. *Algerian Journal of Human Security*, 2(2), 257-277.
10. Ben Berghouth, L. (2023). Al-amn al-saybirānī wa-ḥimāyat khuṣūṣiyat al-bayānāt al-raqmīyah fī al-Jazā'ir fī 'aṣr al-taḥawwul al-raqmī wa-al-dhakā' al-iṣṭinā'ī: al-tahdīdāt, al-tiqnīyāt, al-taḥaddīyāt, wa-ālīyāt al-taṣdī [Cybersecurity and the protection of digital data privacy in Algeria in the era of digital transformation and artificial intelligence: Threats, technologies, challenges, and mechanisms of response]. *State Journal of Social Communication*, 10(1), 443-462.
11. Ben Dhiab, A. M. (2012). *Ḥaqq al-khuṣūṣīyah fī al-tashrī' al-'iqābī al-Jazā'irī* [The right to privacy in Algerian penal legislation] (Unpublished master's thesis). University of Haj Lakhdar, Batna.
12. Centre de Recherche sur l'Information Scientifique et Technique (CERIST). (n.d.). *Accueil*. Retrieved January 24, 2026, from <https://www.cerist.dz/>
13. Constitution of the People's Democratic Republic of Algeria of 1976. (1976). *Official Gazette of the People's Democratic Republic of Algeria*, (94).
14. Eco-Algeria. (2025). *Ittifāqīyat ta'āwun bayna ma'had al-takwīn al-maṣrifī wa-sharikat Kaspersky* [Cooperation agreement between the Banking Training Institute and Kaspersky]. Retrieved February 1, 2026, from <https://mail.eco-algeria.dz/>
15. European Union Agency for Fundamental Rights. (2012). *Handbook on European data protection law*. Publications Office of the European Union. <https://fra.europa.eu/>
16. Jabbour, M. A. (2016). *Al-saybirānīyah hājis al-'aṣr* [Cyberspace: The obsession of the era] (Issue 5). League of Arab States.
17. Jabbour, M. A., & Jabbour, M. (2018). *Al-bayānāt al-shakhṣīyah wa-al-qawānīn al-'Arabīyah* [Personal data and Arab laws] (1st ed.). Arab Center for Legal and Judicial Research, League of Arab States.
18. Law No. 04-15 of November 10, 2004, amending and supplementing Ordinance No. 66-156 on the Penal Code. (2004). *Official Gazette of the People's Democratic Republic of Algeria*, (71).
19. Law No. 06-23 of December 20, 2006, amending and supplementing the Penal Code. (2006). *Official Gazette of the People's Democratic Republic of Algeria*, (86).
20. Law No. 09-04 of August 5, 2009, on specific rules for the prevention and fight against offenses connected with information and communication technologies. (2009). *Official Gazette of the People's Democratic Republic of Algeria*, (47).
21. Law No. 15-04 of February 1, 2015, defining the general rules relating to electronic signature and certification. (2015). *Official Gazette of the People's Democratic Republic of Algeria*, (06).
22. Law No. 15-12 of July 15, 2015, on the protection of the child. (2015). *Official Gazette of the People's Democratic Republic of Algeria*, (39).
23. Law No. 18-07 of June 10, 2018, on the protection of natural persons with regard to the processing of personal data. (2018). *Official Gazette of the People's Democratic Republic of Algeria*, (34).
24. League of Arab States. (2010, December 21). *Arab Convention on Combating Information Technology Offenses*. Cairo.
25. Melouki, S., & Djilali, O. (2025). Al-siyāsah al-'āmmah al-amnīyah al-Jazā'irīyah fī ḍaw' al-taḥaddīyāt al-saybirānīyah al-mu'aṣirah [Algerian public security policy in light of contemporary cyber challenges]. *Journal of Legal and Political Thought*, 9(2), 211-231.
26. Nassakh, F. (2021). Ḥimāyat al-mu'ṭayāt dhāt al-tābi' al-shakhṣī fī ḥill al-'aṣr al-tiknūlūjī wa-al-raqmī wafq al-qānūn 18-7 [Protection of personal data in the technological and digital age according to Law 18-7]. *Journal of Communication and Journalism*, 8(2), 51-69.
27. Ordinance No. 03-05 of July 19, 2003, on copyright and related rights. (2005). *Official Gazette of the People's Democratic Republic of Algeria*, (44).
28. Presidential Decree No. 04-183 of June 26, 2004, establishing the National Institute of Forensic Science and Criminology of the National Gendarmerie and defining its basic law. (2004). *Official Gazette of the People's Democratic Republic of Algeria*, (41).



29. Presidential Decree No. 15-261 of October 8, 2015, defining the composition, organization, and procedures of the National Body for the Prevention and Fight against Offenses Connected with Information and Communication Technologies. (2015). *Official Gazette of the People's Democratic Republic of Algeria*, (53).
30. Presidential Decree No. 20-05 of January 20, 2020, establishing the national system for the security of information systems. (2020). *Official Gazette of the People's Democratic Republic of Algeria*, (04).
31. Presidential Decree No. 20-442 of December 30, 2020, on the issuance of the constitutional amendment approved in the referendum of November 1, 2020. (2020). *Official Gazette of the People's Democratic Republic of Algeria*, (82).
32. Qara, A. (2007). *Al-ḥimāyah al-jazā'iyah lil-ma'lūmātīyah fī al-tashrī' al-Jazā'irī* [Penal protection of information technology in Algerian legislation] (2nd ed.). Dar Houma for Printing, Publishing, and Distribution.
33. Rafi', K. S. (2018). Taqyīd ḥaqq al-ḥuṣūl 'alā al-ma'lūmāt: dirāsah muqāranah [Restricting the right to information: A comparative study]. \*Al-Muhaqqiq Al-Halabi Journal for Legal and Political Sciences, 10\*(2), 87-102.
34. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119, 1-88.
35. TadoSaNews. (2025, May 26). *Ittifāq Jazā'irī Rūsī fī majāl al-amn al-saybirānī* [Algerian-Russian agreement in the field of cybersecurity]. Retrieved February 1, 2026, from <https://tadomsanews.dz/>
36. United Nations. (1948). *Universal Declaration of Human Rights*. General Assembly Resolution 217 A(III).
37. United Nations. (1966). *International Covenant on Civil and Political Rights*. General Assembly Resolution 2200A (XXI).
38. United Nations Office at Geneva. (n.d.). *International Telecommunication Union (ITU)*. Retrieved January 8, 2026, from <https://www.ungeneva.org/>